CRIMINAL JUSTICE CONNECTIONS

An employee publication of the
Texas Department of Criminal Justice

September/October 2014
Volume 22 Issue 1

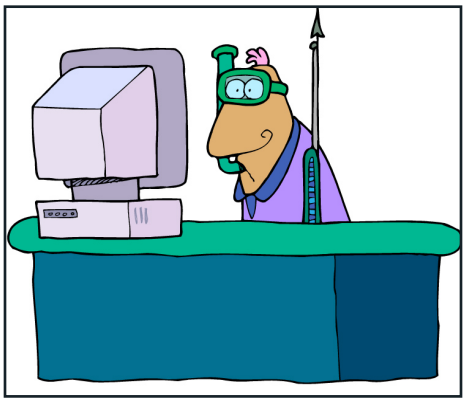
Policies and Benefits

Information Security: phishing attack warning

There has been a recent increase in phishing attempts, a fraud scheme used to gain unauthorized access to confidential information. In this case, agency employees have received emails asking them for their confidential information and threatening to deactivate their account if they refuse to cooperate.

The text of the phishing email reads something like this:

> *Your mailbox has exceeded the storage limit which is set by your administrator. You may not be able to send or receive new mail until you re-validate your mailbox. To re-validate your mailbox please send the following details below:*
>
> *Name:*
> *Username:*
> *Password:*
> *Retype Password:*
> *Email Address:*
> *Phone Number:*
>
> *If you fail to re-validate your mailbox, your mailbox will be deactivated!!!*
>
> *Thanks,*
> *System Administrator*



Be aware that the agency would never send an email request for such confidential information. Also note the exclamation points used to create a sense of urgency so you'll react quickly and without thinking about who might have actually sent this email request, a typical phishing technique. If you believe you might have inadvertently revealed sensitive information, change your password immediately and contact the Information Security Department at (936) 437-1800.

Phishing emails appear to come from a legitimate sender and are used to lure recipients into divulging personal, financial or other sensitive information. Scammers use that information to commit identity theft, gain access to your accounts and hack your computer. Phishers are constantly adapting and improving their techniques, and users must beware of the hidden danger to avoid getting hooked.

Several agency employees receive "spear phishing" attempts each week. Spear phishing targets a particular group within the agency in order to trick recipients into providing confidential information or clicking on attachments or links in order to gain access to a system or data. It is critically important to be vigilant in order to identify and protect yourself from these scams.

Typically, phishing emails use urgent or exciting language to get you to act quickly and without thinking. Tipoffs which help you recognize a phishing attempt include:

- Requests for information like passwords, bank account information, usernames, credit card numbers, Social Security numbers, etc.

- Requests to click on a link which might appear genuine, but which actually directs you to a fake, dangerous site. Learn to recognize fake websites by

Continued on page 2

September/October 2014
Volume 22 Issue 1

Continued from page 1

checking their Web address to see if it's within a legitimate Web domain. For example, if you know that www.bank.com is your bank's legitimate Web domain, beware of similar-looking names like www.Bank-Security.com or www.Bank-Accounts.com; they are likely to be fakes and should not be trusted.

- Attachments that you are directed to open for an urgent reason, or because you will get something of value.

Don't Trust – Verify

You can avoid becoming a cyber fraud victim by taking a few simple anti-phishing precautions, including:

- Never respond to any suspicious email by clicking on links or filling out forms with personal or financial information.

- Don't believe everything you read. If you are unsure as to whether a website is legitimate, confirm it by contacting the company or organization.

- Double check the URLs of websites you visit. Rather than using contact information provided in any email, take a moment and look it up on the company's website.

- Be patient. Too many users become victims of Internet crime because they act on impulse, clicking on a link or an interesting attachment without thinking of the possible consequences.

- Never provide personal information or information about your company or organization via email, text or over the phone.

- Don't open unexpected attachments. Contact the email source to verify the contents. Again, use a trusted source to find contact information for the recipient.